

Privacy Compliance: The Top Ten Steps

1. **Appoint a Privacy Officer**

Privacy laws make organizations accountable to appoint someone to be responsible for privacy compliance.

2. **Learn a little about which privacy laws apply**

Depending on the nature of your business and where you operate, one or more privacy laws may apply to your organization. If you provide services to clients or customers, you may be required by your customers to sign agreements to comply with the privacy laws applicable to them.

3. **Know what your business does with personal information**

Personal information is information about identifiable individuals. It will likely be used in your organization in areas such as human resources, accounting/credit, marketing and sales, client services, shipping and security. It will flow through your business in a variety of ways, on paper and electronically, in archived storage, on forms, in emails and on wireless devices. You may be considering using an online data storage service. Your staff may be using social networking services. You must know how you get personal information, how your organization uses it, how it is disposed of, and how you keep it secure throughout its life cycle.

4. **Get any necessary consents from individuals**

Most privacy laws are consent-based; they require organizations to get consent from individuals before their personal information is collected, used or disclosed. The individual must be told why you require their personal information and what your organization intends to do with it. Consent may be express or implied, depending on the sensitivity of the personal information in the circumstances.

5. Develop privacy policies and practices

You must have written policies for the collection, use, disclosure, retention and disposal of personal information. You must make information about your policies publicly available, through, for example, a brochure or a statement on your website.

6. Review your contracts with third parties

If you use service providers to process your data, or to store records, or for other purposes involving information (including IT providers), you must ensure that they agree to protect the personal information that they deal with on your behalf. If you are a service provider, you will be asked to sign agreements to protect information. Make sure you understand the nature of these promises.

7. Review your practices

You should make sure that your policies and procedures work properly. Errors made by junior staff, inadequate processes or a failure to escalate a problem, can all expose the business to significant risk.

8. Train your staff

The law obliges organizations to ensure that staff is properly trained. To ensure your organization complies with its duties and the privacy policies you've developed, your staff needs to understand how to put your policies into practice, and why it is important to do so.

9. Get ready for access requests

Individuals have a right to access their personal information that your organization holds, by making a request in writing. The law requires you to respond promptly, usually within 30 calendar days. To do this, your staff must be trained to recognize and properly escalate an access request quickly.

10. Be prepared to handle complaints and inquiries

Individuals have a right to complain to you, and if you cannot satisfy them, they can then complain to the Privacy Commissioner. By having an effective complaints resolution process you can deal with individual concerns in an efficient manner and save the costs associated with responding to a more formal complaint or an investigation.

Regardless of the size of your business, your information is a key asset and protecting it is essential to minimize liability and save costs. The Privacy and Freedom of Information practice group has extensive experience assisting clients with all phases of privacy compliance.

For more information contact Sara A. Levine at 604-877-1057 or by email at salevine@alliancelex.com

